U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

September 23, 2014

By E-mail
Joshua L. Dratel, Esq.
2 Wall Street, 3rd Floor
New York, NY 10005

Re: *United States v. Ross William Ulbricht*, 14 Cr. 68 (KBF)

Dear Mr. Dratel:

The Government is in receipt of your discovery requests dated September 17, 2014 (the "September 17 Requests"). As set forth below, the Government objects to the September 17 Requests to the extent they concern the defendant's pending motion for suppression of the contents of the server that hosted the Silk Road website (the "SR Server"). The defense has failed to set forth any valid legal basis for its suppression motion that would support any corresponding discovery requests. Further, the Government objects to the discovery requests to the extent they call for the Government to search for material not in the possession of the prosecution team. Notwithstanding these objections, the Government is producing herewith certain material and information responsive to your requests in the interest of minimizing additional motion practice.

A. Objections

1. Materiality

Federal Rule of Criminal Procedure 16(a)(1) outlines the items subject to disclosure during criminal discovery. Such items include, *inter alia*, "papers, documents, data, photographs, tangible objects . . . or copies or portions of any of these items, if the item is within the government's possession, custody, or control and the item is material to preparing the defense . . . ." Fed. R. Crim. P. 16(a)(1)(E). In the context of this Rule, an item is "material" only if it "could be used to counter the government's case or to bolster a defense." *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir.1993) (internal citations omitted). "Defense" means "the

defendant's response to the Government's case in chief," encompassing only items "which refute the Government's arguments that the defendant committed the crime charged." *United States v. Armstrong*, 517 U.S. 456, 462 (1996) (interpreting predecessor to Fed. R.Crim. P. 16(a)(1)(E)).

"It is defendant's burden to [show] that the documents sought are material to preparing his defense." *United States v. Giffen*, 379 F.Supp.2d 337, 342 (S.D.N.Y.2004) (citation omitted). "Materiality means more than that the evidence in question bears some abstract logical relationship to the issues in the case. There must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." *Id.* (internal quotation marks omitted). A showing of materiality cannot be made through conjecture or conclusory allegations. *Id.* Moreover, evidence is not material merely because it might be "'useful' in order [for a defendant] to meet [his] burden under Rule 16(a)(1)(E)" to obtain further discovery. *United States v. Rigas*, 258 F.Supp.2d 299, 307 (S.D.N.Y. 2003). In short, in contrast to civil discovery, criminal discovery is not exploratory. Only if a defendant can show at the outset how the requested materials will advance his defense to the Government's case-in-chief is he entitled to their disclosure.

In light of these basic legal principles, the Government objects to the September 17 Requests as a general matter on the ground that no adequate explanation has been provided as to how the requested items are material to the defense. Most of the requests appear to concern how the Government was able to locate and search the SR Server. Yet the Government has already explained why, for a number of reasons, there is no basis to suppress the contents of the SR Server: (1) Ulbricht has not claimed any possessory or property interest in the SR Server as required to establish standing for any motion to suppress; (2) the SR Server was searched by foreign law enforcement authorities to whom the Fourth Amendment does not apply in the first instance; (3) even if the Fourth Amendment were applicable, its warrant requirement would not apply given that the SR Server was located overseas; and (4) the search was reasonable, given that the FBI had reason to believe that the SR Server hosted the Silk Road website and, moreover, Ulbricht lacked any expectation of privacy in the SR Server under the terms of service pursuant to which he leased the server.

Particularly given these circumstances, it is the defendant's burden to explain how the contents of the SR Server were supposedly obtained in violation of the defendant's Fourth Amendment rights and how the defendant's discovery requests are likely to vindicate that claim. The defense has failed to do so, and the Government is unaware of any evidence – including any information responsive to the defense's discovery requests – that would support any viable Fourth Amendment challenge. Instead, the defense's discovery requests continue to be based on mere conjecture, which is neither a proper basis for discovery nor a proper basis for a suppression hearing. *See United States v. Persico*, 447 F. Supp. 2d 213, 217 (E.D.N.Y. 2006) ("basing discovery requests on nothing more than mere conjecture" is a "non-starter"); *United States v. Seijo*, No. 02 Cr. 1415, 2003 WL 21035245, at *4 (S.D.N.Y. May 7, 2003) ("A defendant seeking the suppression of evidence is not automatically entitled to an evidentiary hearing on his claim; rather, the defendant must first 'state sufficient facts which, if proven, would [require] the granting of the relief requested.'") (quoting *United States v. Kornblau*, 586 F.Supp. 614, 621 (S.D.N.Y.1984)). In the absence of any cognizable legal basis for the

defendant's suppression motion, the Government does not believe the defense is entitled to any discovery with respect to the motion.

2. Prosecution Team

The Government also objects to the unbounded definition of the term "government" set forth in the September 17 Requests. Specifically, the requests ask the prosecution to search for information within "not only the United States Attorney's Office for the Southern District of New York, but also the Offices in all other Districts, any and all government entities and law enforcement agencies, including but not limited to the Federal Bureau of Investigation, Central Intelligence Agency, Drug Enforcement Administration, Immigration and Customs Enforcement Homeland Security Investigations, National Security Agency, and any foreign government and/or intelligence agencies, particularly those with which the U.S. has a cooperative intelligence gathering relationship, *i.e.*, Government Communications Headquarters ("GCHQ"), the British counterpart to the NSA."

Even in the *Brady* context, the law is clear that a prosecutor has a duty to learn only of "evidence known to . . . others acting on the government's behalf in the case." *Kyles v. Whitley*, 514 U.S. 419, 437 (1995); *see United States v. Payne*, 63 F.3d 1200, 1208 (2d Cir. 1995). The imposition of an unlimited duty on a prosecutor to inquire of other offices and agencies not working with the prosecutor's office on the case in question would inappropriately reflect a "monolithic view of government that would "condemn the prosecution of criminal cases to a state of paralysis." *United States v. Gambino*, 835 F. Supp. 74, 95 (E.D.N.Y. 1993), *aff'd*, 59 F.3d 353 (2d Cir. 1995). Accordingly, the Second Circuit and courts within it have repeatedly concluded that the prosecution team cannot be deemed to have constructive knowledge of evidence possessed by other government agencies not involved in its investigation of the defendant. *See, e.g.*, *United States v. Avellino*, 136 F.3d 249, 256 (refusing to impute to federal prosecutor information gathered in state investigation); *Pina v. Henderson*, 752 F.2d 47, 49-50 (2d Cir. 1985) (concluding prosecution did not have constructive knowledge of information relayed to parole officer); *United States v. Stofsky*, 527 F.2d 237, 243-44 (2d Cir. 1975) (no imputation of witness's tax information held by the IRS); *United States v. Canniff*, 521 F.2d 565, 573-74 (2d Cir. 1975) (no imputation of information in witness's Pre-Sentence Report that was not in the government's possession); *United States v. Chalmers*, 410 F. Supp. 2d 278, 289-90 (S.D.N.Y. 2006) (refusing to impute evidence in custody of federal agencies that did independent investigation of United Nations Oil-For-Food program to prosecution team).

B. Responses

Without waiving the objections set forth above, in the interest of minimizing any additional motion practice, the Government hereby provides the following responses to the September 17 Requests, based on the information available to the prosecution team:

1. The MD5 hash value of the device mapper for the partition sda4_crypt as well as the MD5 hash of the RAW (.dd) image of the partition, both of which should have been generated, when the following command was issued (according to the bash history attributable to the FBI): 2175 date ; md5sum /dev/mapper/sda4_crypt >

/media/sv_13_0210/evidence/l1c1_sda4_crypt/sd4_md5.txt ; date ; md5sum /media/sv_13_0210/evidence/l1c1_sda4_crypt/sda4_crypt.dd > /media/sv_13_0210/evidence/l1c1_sda4_crypt/sda4_crypt.dd.md5.txt.

The commands referenced were unsuccessful and did not return an MD5 hash. The Government is not in possession of an MD5 value with regard to the "device mapper for partition sda4_crypt." After the image was completed, an MD5 value was created for the raw .dd image. The hash value returned was 1e610e4a5f28b3d01bb8efd835ef0fed.

2. Any and all logs of communications between the front-end and back-end Silk Road Servers.

If by "front-end" server you mean the server hosting the Silk Road hidden service and "back-end" server you mean the server hosting the Silk Road website, then the Government is not aware of logs of communications between the two other than any logs included on the images of the servers already provided to you in discovery.

3. Any and all traffic and communication logs for the Icelandic server assigned IP address 193.107.84.4.

The Government has already provided these records to you.

4. Exact dates and times of access and/or attempted access to the Silk Road servers by former SA Tarbell and/or CY-2.

Please see Attachment 1, which is an excerpt of a log file on the SR Server, reflecting the IP address used by former SA Tarbell to directly contact the SR Server outside of Tor, as described in the fourth sentence of paragraph 8 of the Tarbell Declaration. The log file from which this excerpt is taken is found on the image of the 193.107.86.49 server ("orange21.tar" file) at /home/s/oldlogs/access.log.3.gz [6/11/2013:16:58:36 +0000].

5. The name of the software that was used to capture packet data sent to the FBI from the Silk Road servers.

Other than Attachment 1, the Government is not aware of any contemporaneous records of the actions described in paragraphs 7 and 8 of the Tarbell declaration. (Please note that Attachment 1 is marked "Confidential" and is subject to the protective order entered in this matter.)

6. A list of the "miscellaneous entries" entered into the username, password, and CAPTCHA fields on the Silk Road login page, referenced in the SA Tarbell's Declaration, at ¶ 7.

See response to request #5.

7. Any logs of the activities performed by SA Tarbell and/or CY-2, referenced in ¶ 7 of SA Tarbell's Declaration.

See response to request #5.

8. Logs of any server error messages produced by the "miscellaneous entries" referenced in SA Tarbell's Declaration.

See response to request #5.

9. Any and all valid login credentials used to enter the Silk Road site.

See response to request #5.

10. Any and all invalid username, password, and/or CAPTCHA entries entered on the Silk Road log in page.

See response to request #5.

11. Any packet logs recorded during the course of the Silk Road investigation, including but not limited to packet logs showing packet headers which contain the IP address of the leaked Silk Road Server IP address [193.107.86.49].

See response to request #5.

12. Any server configuration files from the time period referenced in the Tarbell Declaration, at ¶ 7, including in particular, NGINX vhost configuration files obtained from the Silk Road Server in early June 2013.

Any server configuration files from the SR Server in the Government's possession are contained in the images of the SR Server already provided to you. Those images were created in late July 2013 and early October 2013.

13. Any and all data obtained from pen registers judicially authorized in this case.

The Government has provided all available pen register data used to detect Ulbricht's email and Internet activity in September 2013, as well as pen register data received from Icelandic law enforcement authorities concerning the SR Server and the server described in the Tarbell Declaration as Server-1. To the extent any other pen register information was obtained in the course of the investigation, the Government objects to this request on the ground that such information is not material to the defense or otherwise required to be produced under Rule 16.

14. Information and documentation regarding how the IP address (193.107.84.4) of the initial Silk Road Server was obtained.

The Government objects to this request on the ground that it is not material to the defense. As noted in the Tarbell Declaration, although the Government originally asked Icelandic authorities for assistance with respect to this server – including obtaining subscriber information, collecting routing information, and covertly imaging the server – Icelandic authorities did not produce traffic data for Server-1 until May 2013. Thereafter, on June 12, 2013, the Government informed Icelandic authorities that it believed that the SR Server was now hosting the Silk Road website, and thus requested that Icelandic authorities search the SR Server instead. However, Icelandic authorities had already imaged the contents of Server-1 by this time, on or about June 6, 2013. Although the Government did not ask Icelandic authorities to share the image of Server-1, Icelandic authorities included the image on the same device on which it produced the image of the SR Server to the Government on or about July 29, 2013. The Government does not intend to use any contents from Server-1 at trial, and accordingly the Government objects to this request as immaterial.

15. Any and all correspondence between the Reykjavik Metropolitan Police and the United States government (as described in fn. 1).

The Government reasserts its general materiality objections set forth above. The only potential relevance of the requested correspondence is to the issue of whether U.S. officials had "authority to control or direct" the actions of the Reykjavik Metropolitan Police ("RMP") with regard to their search of the SR Server. *United States v. Getto*, 729 F.3d 221, 231 (2d Cir. 2013). The Government does not believe that the requested correspondence, which concern requests for foreign law enforcement assistance, would establish that U.S. officials had such authority. *See id.*, 729 F.3d at 230-31 (holding that the Fourth Amendment does not apply to actions of foreign officials merely because they undertook investigative steps only in response to an American MLAT request). But in any event, even if the facts could demonstrate that U.S. officials had "authority to control or direct" the actions of the RMP, the defendant has not articulated any viable theory of how the RMP's search violated his Fourth Amendment rights. Because the defendant has failed to assert any theory, let alone facts, that would establish such a violation, there is no justification for the defense to obtain wide-ranging discovery into the Government's communications with foreign law enforcement authorities. Collecting, reviewing, and producing the requested correspondence would not only be burdensome for the Government, but also, were such correspondence routinely subject to disclosure in any investigation involving international cooperation, candid and effective communications between foreign and U.S. law enforcement authorities would be inhibited. *Cf. United States v. Getto*, 729 F.3d 221, 230 (2d Cir. 2013) (citing *United States v. Morrow*, 537 F.2d 120, 140 (5th Cir.1976) ("Normal lines of communication between the law enforcement agencies of different countries are beneficial without question and are to be encouraged."); *cf. also United States v. Cherry*, 876 F. Supp. 547, 551-52 (S.D.N.Y. 1995) (rejecting request for discovery of investigative files of local law enforcement agency that cooperated with federal government in its investigation, finding that subjecting such materials to discovery "would in all likelihood inhibit cooperation between local and federal law enforcement agencies, to the benefit of criminals but to the detriment of the public good"). To the extent the Court determines, however, that it needs to resolve the question

of whether U.S. officials had "authority to control or direct" the actions of the RMP, the Government would propose to submit the requested correspondence to the Court *ex parte* for its review, in light of the Government's concern about the sensitivity of its communications with foreign law enforcement authorities.

16. A copy of the August 27, 2013, First Supplemental Request issued by U.S. Authorities to Icelandic Authorities.

The Government objects to this request on the ground that it is not material to the defense, particularly because the First Supplemental Request does not concern the SR Server or any other evidence the defendant seeks to suppress.

17. The September image of the 193.107.86.49 server, referenced in item #9 of the government's March 21, 2014, discovery letter.

The SR Server was originally imaged in July 2013. The Government is not aware of any image of the SR Server made by Icelandic authorities in September 2013. As far as the Government is aware, the SR Server was re-imaged by Icelandic authorities in October 2013 pursuant to an official U.S. request made in late September 2013 (which has been produced to you). This image was produced to you as item #12 in the Government's March 21, 2014 discovery production. To the extent that the Government's cover letter accompanying this production also references the server image in item #9, this appears to be an error.

18. In regard to the several .tar compressed archives (all.tar; home.tar; and orange21.tar) produced as part of item #1 of the government's March 21, 2014, discovery letter, please (a) identify when these .tar archives were created; (b) list the commands that were issued to create them; (c) state whether any cryptographic hash values were generated for the .tar archives at the time they were created.

(a) The creation dates of these archive files are reflected in their file properties.

(b) According to information provided by the RMP, copying of the data was executed as follows:

1. Screen and keyboard are connected to the machine and restart it with ctrl + alt + del
2. Booted console in Single mode with bash shell to bypass password authentication (init = / bin / bash)
3. Copying machine with the following command line anti: tar-cvpzf / mnt/orange21.tar.gz-exclude = / mnt - exclude = / proc-exclude = / sys-exclude = / dev-exclude = / run /
4. USB Disk un-mounted and console rebooted and linked back to the network.
5. The machine boots back up normally.

(c) The Government is unaware of any records in its possession responsive to this request.

Sincerely,

PREET BHARARA
United States Attorney

By: _____
Serrin Turner
Assistant United States Attorney

Enclosures